Data Access Policy

Approved by the University Council on December 17, 2021
Approved by the Executive Committee of the BOT on February 22, 2022
Approved by the Board of Trustees on July 15, 2022

In pursuit of the University mission focused on higher education, research, and community engagement, University community members often have the need to access, collect, modify, or create Institutional data. As such, this data is considered an important University asset that needs to be properly managed and protected. The main aim of this policy is to ensure the availability of Institutional data to appropriate users while highlighting the shared responsibility of these users in maintaining institutional data security, privacy, confidentiality, and integrity as applicable.

Towards that aim, Institutional data is defined as information stored in print or electronic format that is used in support of the functions of the Institution (University), by members of the University community, including administrators, faculty members, staff, students, alumni, guests, and visitors. The present policy is developed with the ultimate objective of gearing the system towards digital data and minimizing the print format to the maximum extent possible.

1. Compliance with Laws, Rules, and Regulations

The University community members accessing Institutional data are required to comply with the pertinent rules and regulations set by the University and all applicable University policies aiming to establish information security and protect sensitive and critical information. In addition, University community members are required to comply with all applicable national laws including, but not limited to, the Code of Obligations and Contracts, 1932 (قانون الموجبات والعقود، 1932), the Right to Access Information Act, 2017 (قانون حق الوصول إلى المعلومات، 2017), the Medical Ethics Act, 1994 (قانون الآداب الطبّية، 1994), and the E-Transaction and Data Protection Act, 2018 (قانون المعاملات الالكترونية والبيانات ذات الطابع الشخصي، 2018).

2. Classification of Data Stakeholders

The community members dealing with data at NDU are classified into five groups:

A. **Data Trustee:** is the President and, by delegation, the Vice-Presidents of the University, entrusted by the University, the sole owner of Institutional data, to oversee the implementation of this policy in their respective operational areas.

B. **Data Stewards:** are University officials, typically at the level of the Registrar, Deans, or Directors of various University units, who have the responsibility of implementing this Data Access Policy for data under their stewardship and under the supervision of the appropriate Data Trustee. They might collect, update, process, and use data with the support of the Data Curator.

C. **Data Curator:** is the Office of Institutional Research and Assessment (OIRA), which reconciles and correlates the data as well as processes and manages data requests. When authorized by the appropriate Data Steward, the Data Curator makes the relevant Institutional data available to requesters.

D. **Data Custodian:** is the Office of Information Technology (OIT) which coordinates with the Data Curator, the Data Stewards, and the Data Trustees to develop and manage the software applications/interfaces used to create, update, integrate, and provide access to the data and maintains the computer hardware systems where the Institutional data are stored.

E. **Data Users:** are University community members or external stakeholders who use Institutional data as part of their job-related functions or for other University approved purposes (e.g. students using institutional data for research).

3. Categorization of Data

Depending on its level of sensitivity and criticality and on its legal protection status, Institutional data is classified into three categories:

A. **Restricted Data –** This category represents the data protected by law or considered as confidential by the Data Stewards. Protected health information is an example of restricted data.

B. **Limited Access Data –** This category is the default data category deemed by the corresponding Data Steward to be inappropriate for public use. It is made available only to a specific group of University community members based on a need-to-know basis. University general finance records are examples of limited access data.

C. **Public Data –** This category represents all data that is widely available for public use with no restrictions. The volume of this category of data is to be properly managed through the reduction of unnecessary limitations in line with the principles of transparency and data availability. Examples of this category of data are the credit cost and program details.

The classification of data as well as the definition of access privileges is the sole responsibility of the Data Stewards in coordination with the concerned Data Trustees. Every time a data set is created, the concerned Data Steward must categorize it as per the above A, B and C categories and list the associated access privileges. The categorization and access privileges have to be further approved by the corresponding Data Trustee prior to making the data official.

4. Responsibilities of Data Trustees

Data Trustees are the University officials to whom the Institutional data is entrusted. In this capacity, each Data Trustee is directly responsible for the types of data existing or collected/generated in his or her operational area. However, Data Trustees may delegate parts of this responsibility whenever deemed appropriate, as follows:

A. The planning and policy development part of this responsibility may be collectively delegated by Data Trustees to an Ad-hoc Data Access Steering Committee to be appointed by the President on an a need basis.

B. The policy implementation may be delegated by Data Trustees to his/her own Data Stewards.

In addition, Data Trustees have supervisory and approval responsibilities towards their corresponding Data Stewards or potential Steering Committees in relation to policy implementation and the development of related processes and procedures.

5. Responsibilities of Data Stewards

Data Stewards are the University officials delegated by Data Trustees to implement the data access policy in their own operational areas through the establishment and execution of procedures or processes targeting various functions including:

A. Data categorization: given a default category of limited access, the Data Steward categorizes each type of data in his/her own operational area based on privacy and confidentiality requirements, legal requirements, or criticality considerations.
B. Assignment of data access privileges to Data Users operating under their stewardship. Data Users granted authorizations to use limited access or restricted data are to be formally notified of their privileges and the corresponding responsibilities.
C. Decision making regarding the approval/denial of requests for access to limited access or restricted data in coordination with the corresponding Data Trustee.
D. Establishment and implementation of procedures and processes in coordination with the Data Curator including protection and control procedures, the generation of periodic data views, and the execution and authentication of data access privileges.

6. Responsibilities of Data Users

When working with Institutional data, all Data Users are required to use the data only for the purpose of accomplishing their functions and to protect their authorization privileges through various means including:

A. Not disclosing or distributing institutional data except as required by their job descriptions and after seeking the approval of the appropriate Data Steward.
B. Not using any institutional data for personal gain, profit or interest, or for the personal gain, profit, or interest of others.
C. Complying with all applicable laws, rules, and regulations relating to authorized and proper access, use, or disclosure of information (intentional and non-intentional), and observing ethical standards relating to the privacy and confidentiality of individuals whose records they access.

7. Responsibilities of the Data Curator

The Data Curator is the Office of Institutional Research and Assessment (OIRA), which is assigned the central role of handling all data requests and securing the proper approvals prior to releasing the data to users. The Data Curator establishes and implements various functions including:

A. Ensuring the integrity and high quality of Institutional data made available to users by making certain this data has a high standard of accuracy, consistency, completeness (non-selectivity), and timeliness.
B. Generating data views in coordination with Data Stewards and Data Trustees whenever needed and with the support of the Data Custodian.
C. Maintaining a dictionary or a catalog of definitions for all data fields as well as data aggregation tools in collaboration with the Data Custodian.

8. Responsibilities of the Data Custodian

The Data Custodian is the central unit in charge of storing, protecting, and maintaining, institutional data in all electronic formats. Its role is particularly critical in the establishment, monitoring, and support of data security. The Data Custodian establishes and implements various procedures and processes targeting a number of functions including:

A. Developing and managing the software applications/interfaces used to create, update, integrate, and access the data in coordination with Data Stewards and the Data Curator.
B. Storage, maintenance, and support of institutional data in electronic formats originating from various administrative, support, and academic units.
C. Establishment and deployment of a high security system for the purpose of preventing unauthorized access to data particularly restricted and limited access data. Such a system may include, but not limited to, security-related rules, regulations, processes, and procedures such as protection and control procedures, encryption of restricted data, and safe computing standards among others.
D. Activation, authentication, monitoring, and termination of data access privileges as requested by the concerned Data Stewards or Data Trustees.

9. Responsibilities of the Data Access Steering Committee (DASC)

The Ad-hoc Data Access Steering Committee (DASC) is a committee appointed by the University President for the purpose of planning and policy development whenever needed. DASC members are typically selected by the President from Data Trustees and Data Stewards, a representative of the Data Curator, a representative of the Data Custodian, and other concerned professionals. The main task of the committee is to periodically update, amend, and develop the Data Access Policy in coordination with all Data Trustees and Data Stewards.

10. Special Protection of Restricted and Limited Access Data

Whereas the principle of data availability and data integrity are typically applied to all institutional data including public data, the principles of data security, privacy, and confidentiality should be particularly applied with restricted and limited access data. To that end, all data users are expected to handle restricted and limited access data with utmost care and attention, apply safe computing standards, and follow appropriate guidelines and procedures. These procedures include the following:

A. Protection of restricted and limited access data through encryption or alternative methods, as applicable, if this data is stored or used on portable devices, are transmitted electronically, or physically moved from their secure University locations.
B. Prevention of storage of restricted data on personally owned computers or storage devices.
C. Prevention of storage or use of restricted or limited access data by external stakeholders without contractual agreements providing the same level of protection and control adopted at the University.

11. Handling Requests for Access to Restricted or Limited Access Data

All requests for access to restricted or limited access data whether by University internal stakeholders (administrators, faculty members, staff, or students) or external stakeholders (alumni, guests, visitors, or other parties) must be handled with extreme care. Such requests must be addressed in writing using the attached “Data Request Form” to the Data Curator, who, in coordination with the concerned Data Stewards, should assess it based on the existence of a need-to-know basis and on the criticality of the requested data. The decision of the Data Steward should be authenticated by the corresponding Data Trustee.

In case of denial of the request, the reasons for the denial should be explained in writing to the requester. In this case, the data requester may appeal the decision through the proper appeal channels available at the University.

12. Reporting of Breaches and Violations

Actual or suspected breaches of this Data Access Policy, in particular, unauthorized access or improper disclosure of restricted or limited access data, and/or violations of pertinent University rules and regulations, and/or violations of relevant national legal obligations must be reported to the Data Curator and the appropriate Data Steward/Trustees, where applicable.

13. Enforcement

Breaches of this Data Access Policy and associated rules, regulations, processes, and procedures will be handled according to the existing University disciplinary procedures. Related violations of local laws or regulations will be reported to the local authorities as required by law.

Drafted by the Ad-hoc Data Access Policy Committee: *Summer 2019* (based on a draft by the Data Access Steering Committee, 2011)

Notre Dame University-Louaize
Data Request Forms
Draft - Version 2.0

Data stored in the University is an Institutional resource. This data is made available to predefined individuals on a need-to-know basis. The user agrees to make responsible and ethical usage of the data in cooperation with the Data Curator. External users may request data access by filling in the enclosed form and submitting it to the Data Curator, i.e. the Office of Institutional Research and Assessment (OIRA), by e-mail at oira@ndu.edu.lb. Internal users may submit similar requests using the shorter form enclosed at the end. The Data Curator is in charge of securing the proper approvals to release the data and answering all requests with the related outcomes. In case the user request is declined, an appeal may be forwarded through the proper appeal channels in place at the University.

Since some data are limited or restricted and may be sensitive, and the release of such data could bring harm to the institution or its community, an additional signature is required upon receiving the data showing details of the use.

Notre Dame University-Louaize (NDU)

Office of Institutional Research and Assessment (OIRA)

Data Request Form for External Users

Please fill out sections A-E of this form completely and accurately. Incomplete forms cannot be processed. You may attach additional sheets if more space is needed.

A. Contact Information

First Name: Last Name:

E-mail:

Phone:

Affiliation Institution/Company:

Address:

B. Data Request Details:

Describe in as much details as possible your data request and the intended use of data:

C. Data Handling

Will data be used in presentations or publications? □ Yes□ No

If yes, where and when will this data be presented and/or published?

How and for how long will the data be stored?

Who will have access to the data?

D. Data Format Details:

List possible formats for the data requested (please note that some formats may not be available):

□ Any Format Available
□ MS Office (Excel, …)
□ PDF and similar print-ready formats
□ Other, Please Specify: ____

E. Signature:

□ I accept to use the data solely for the data request described in section B above.

Name and Signature Date

F. For Office Use Only

Data Request Approved: □ Yes□ No

Date Request Received: __________________ Date Completed:_________________

If No, provide explanations and reasons for rejection:

Name and Signature Date

Notre Dame University-Louaize (NDU)

Office of Institutional Research and Assessment (OIRA)

Data Request Form for Internal Users

Please fill out sections A-D of this form completely and accurately. Incomplete forms cannot be processed. You may attach additional sheets if more space is needed.

A. Contact Information

Name:

Faculty/Office: Department:

B. Data Request Details:

Describe your data access request and the intended use of data:

C. Data Format Details:

List possible formats for the data requested (please note that some formats may not be available):

□ Any Format Available
□ MS Office (Excel, …)
□ PDF and similar print-ready formats
□ Other, Please Specify: ____

D. Signature:

□ I accept to use the data solely for the data request described in section B above.

Name and Signature Date

E. For Office Use Only

Data Request Approved: □ Yes□ No

Date Request Received: __________________ Date Completed:_________________

If No, provide explanations and reasons for rejection:

Name and Signature